UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/725,821	11/29/2000	James D. Dworkin	SC11015ZC	4735

23125 7590 09/07/2005

FREESCALE SEMICONDUCTOR, INC.
LAW DEPARTMENT
7700 WEST PARMER LANE MD:TX32/PL02
AUSTIN, TX 78729

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/725,821
Filing Date: November 29, 2000
Appellant(s): DWORKIN ET AL.

James L. Clingan, Jr.
Reg. No. 30,163
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 6/24/2005.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Prior Art of Record

6,708,273	OBER	3-2004
5,623,545	CHILDS	4-1997
4,896,296	TURNER	1-1990

4,314,349	BATCHER	2-1982
4,739,195	MASAKI	4-1988
4,399,517	NIEHAUS	8-1983

Schneier, "Applied Cryptography", 1996, John Wiley and Sons, 2nd Edition, pp. 436-441

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-7, 14-15, and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ober et al. (U.S. Patent Number 6,708,273) hereinafter referred to as Ober, in view of Childs et al. (U.S. Patent 5,623,545) hereinafter referred to as Childs, Schneier (Applied Cryptography) hereinafter referred to as Schneier, Turner et al. (U.S. Patent Number 4,896,296) hereinafter referred to as Turner, and further in view of Batcher (U.S. Patent Number 4,314,349) hereinafter referred to as Batcher.

Regarding claim 1, Ober disclosed an integrated circuit for performing security functions including the SHA-1 and MD5 hash algorithms (See Ober Figure 1 Element 30). However, Ober failed to disclose an embodiment for the implementation of the two hash functions.

Childs teaches a hardware implementation of the SHA-1 algorithm. The implementation includes five registers for storing chaining variables as called for by the SHA-1 algorithm (See Childs Fig. 5 elements 508-512). Childs teaches a function circuit receiving chaining variables B, C, and D (See Childs Fig. 5 Element 516). Childs also teaches a summing circuit (Elements 520-523) receiving the output of the function circuit (f_e) and the fourth chaining variable (E) and the output coupled to the register file through a multiplexer (Element 507) (See Childs Fig. 5).

Schneier teaches that the MD5 algorithm has the same elements shown above for the SHA-1 algorithm, except that there is not a fifth chaining variable 'E' as in SHA-1 (See Schneier Page 438 Fig. 18.6).

Turner teaches that by using a multiplexer, with one input set to zero, the other inputs can be selectively excluded from the input to another function (See Turner Col. 7 Paragraph 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Childs and Schneier in the invention of Ober in order to carry out the hashing functions. This would have been obvious because one of ordinary skill in the art would have been motivated to provide the full functionality of the IPSec protocol when implementing this protocol.

It also would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Turner in the combination of Ober, Childs, and Schneier in order to selectively exclude the fifth chaining variable (E) from the inputs to the summing circuit in such a manner that when SHA-1 is being performed, the fifth chaining variable is passed through the multiplexer, and when MD5 is being performed, the zero is passed through the multiplexer. This would have been obvious because one of ordinary skill in the art would have been motivated to utilize the multiplexer in order to minimize the elements in the circuit of Ober, as evidenced by Batcher (See Batcher Col. 6 Paragraph 3).

Claim 2 recites a barrel shifter, coupled to an adder, coupled to a multiplexer, all coupled to the output of the summing circuit. MD5 requires a shifter and adder coupled to the output of the summer, as can be seen in the two rightmost elements of figure 18.6 (See Schneier Page 438). Claim 2 further recites the other input of the multiplexer being coupled to the output of the summing circuit. SHA-1 does not require the shifter or the adder at the output of the summing circuit.

It would have been obvious to employ the teachings of Batcher in order to multiplex the elements of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

Claim 3 recites a third multiplexer coupled to the output of the second multiplexer and also coupled to the register file to receive a fifth chaining variable (A). Childs disclosed that chaining variable B had input from chaining variable A during SHA-1 (See Childs Fig. 5 Elements 508 and 509). Schneier disclosed that chaining variable B had input from the result of the adder (See Schneier Page 436 Paragraph 9 – Page 437 Paragraph 1).

Claim 3 further recites a fourth multiplexer coupled to the output of the second multiplexer and to the register file for receiving the third chaining variable (D). Childs disclosed that chaining variable A had input from the summing circuit during SHA-1 (See Childs Fig. 5 Elements 507, 508, and 523). Schneier disclosed that chaining variable A was coupled to the chaining variable D (See Schneier Page 437 Lines 18-21).

It would have been obvious to employ the teachings of Batcher in order to multiplex the elements of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

Claims 4-5 were inherent in the combination of Ober, Childs, Schneier, Batcher and Turner, in order for proper operation of the MD5 and the SHA-1 when each was selectively performed in Ober. This was inherent because the MD5 algorithm must have received the correctly multiplexed inputs for MD5 and the SHA-1 must have received the correctly multiplexed inputs for SHA-1 in order for the hashes to be calculated correctly.

Regarding claim 6, Childs disclosed a shift circuit and a fifth multiplexer for selectively shifting the second chaining variable (B) for input to the third chaining variable (C) (See Childs Fig. 5 Elements 509, 518, 517, and 510).

Regarding claim 7, Childs disclosed a shift circuit receiving chaining variable A and outputting to the summing circuit in accordance with SHA-1 (See Childs Fig. 5 Elements 508, 519, 520, and 522). Schneier disclosed chaining variable A being input to the summing circuit in accordance with MD5 (See Schneier Figure 18.6).

It would have been obvious to employ the teachings of Batcher in order to multiplex the elements of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

Claim 14 recites a register file for storing five chaining variables, in which the five variables are preloaded for each of two algorithms. Childs depicted a register file for storing five chaining variables (See Childs Fig. 5 Elements 508-512) and also disclosed loading the registers with preset values at the beginning of the SHA-1 algorithm (See Childs Fig. 5 Element 507 and Col. 1 Lines 25-32). It was inherent in the combination of Ober, Childs, Schneier, Batcher and Turner, that when MD5 was being performed, the initial MD5 variables were loaded into the register file (See Schneier Page 436 Lines 33-38).

Claim 14 further recites a function circuit receiving three of the chaining variables and producing a logical value dependant on the algorithm being performed. Childs disclosed a function circuit taking three chaining variables and producing a logical value for the SHA-1 algorithm (See Childs Fig. 5 Element 516). Schneier disclosed a function, for the MD5 algorithm, which took three chaining variables and produced a logical output (See Schneier Page 437 Lines 5-11). These functions are different for SHA-1 and MD5 (See Childs Col. 1 Table at Line 20 and Schneier Page 437 Lines 5-11).

Claim 14 also recites a storage element for providing a set of constants for each algorithm to a summing circuit, and the summing circuit also receiving the output of the function circuit (See rejection of claim 8 regarding the storage circuit).

Claim 15 recites a register array, with a plurality of registers and a decoder circuit for selecting a word from the register array for the first algorithm (See Childs Fig. 6 Elements 602, and 603 and Schneier Page 437 Line 16 – Page 440 Line 17).

Claim 17 recites an output of the array being supplied from a word-wise circular queue when computing a second algorithm (See Childs Fig. 6 Element 602, 603, and 604).

Claim 18 recites the first algorithm being MD5 and the second algorithm being SHA-1. Schneier disclosed the first algorithm being MD5 (See Schneier Page 436) and Childs disclosed the second algorithm being supplied by FIPS PUB 180-1 (See Childs Abstract), which is the SHA-1 algorithm.

Claims 8-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ober, Childs, Schneier, Turner, and Batcher, as applied to claim 1 above, and further in view of Niehaus et al (US Patent Number 4,399,517) hereinafter referred to as Niehaus.

Regarding claim 8, the combination of Ober, Childs, Schneier, Turner, and Batcher disclosed a storage circuit (See Childs Fig. 5 Element 515), a register array providing W_t (See Childs Fig. 5 Element 514), a register file for storing chaining variables A-E (See Childs Fig. 5 Elements 508-512), and a summing circuit (See Childs Fig. 5 Elements 520-523) receiving constants from the storage circuit (See Childs Fig. 5 Elements 515 and 520), one input coupled to the register array (See Childs Fig. 5 Elements 514 and 520), one input coupled to either chaining variable A or a shifted version of chaining variable A depending on the mode of operation (See rejection for claim 7 above), one input for receiving a logical function in accordance with chaining variables 1, 2, and 3 (See Childs Fig. 5 Element 516), and one input providing a fourth chaining variable or a zero depending on the mode of operation (See rejection of claim 1 above).

The combination of Ober, Childs, Schneier, Turner, and Batcher further disclosed the storage circuit storing two sets of constants, one for SHA-1 and one set for MD5. Childs disclosed storing the set K_t for SHA-1 (See Childs Fig. 5 Element 515 and Col. 8 Paragraph 3) and although Schneier did not

specifically disclose storing the constants for MD5, it was inherent that they were stored in order to have performed the 64 steps in the four rounds as required by the MD5 algorithm (See Schneier Pages 438-440 t_i).

It would have been obvious to employ the teachings of Batcher in order to multiplex the constants of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

However, the combination of Ober, Childs, Schneier, Turner, and Batcher failed to disclose the summing circuit being an adder.

Niehaus teaches a multiple input adder, which takes up to six inputs and provides the sum of the inputs (See Niehaus Abstract), and the advantages of this adder (See Niehaus Col. 1 Lines 41-48).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Niehaus in the Hash Block of the combination of Ober, Childs, Schneier, Turner, and Batcher by providing the multiple input adder in place of the summing circuit. This would have been obvious because the ordinary person skilled in the art would have been motivated to minimize gate delay as well as the fan in of the inputs.

Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ober, Childs, Schneier, Turner, and Batcher as applied to claim 15 above, and further in view of Masaki (US patent Number 4,739,195).

The combination of Ober, Childs, Schneier, Turner, and Batcher disclosed the register array forming a word wise circular queue (See Childs Fig. 6 Elements 602, 603, 605, 608, and 601), an exclusive-OR receiving four data words from the register file (See Childs Fig. 6 Elements 603, 605, and 606), and a shift register coupled to the output of the exclusive-OR for providing input to the register file (See Childs Fig. 6 Elements 605, 607, 608, 601, and 602). The combination of Ober, Childs, Schneier, Turner, and Batcher disclosed the shift being a one-bit shift (See Childs Abstract). However, the

combination of Ober, Childs, Schneier, Turner, and Batcher failed to disclose that the data words received by the XOR were received simultaneously.

Masaki teaches that instead of using a two input XOR to XOR four inputs, a four input XOR gate can be used to provide the output in less time (See Masaki Col. 1 Lines 9-24).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Masaki in the Hash Block of the combination of Ober, Childs, Schneier, Turner, and Batcher by using a four input XOR gate instead of the two input XOR gate of Childs in order to XOR the four data words. This would have been obvious because ordinary person skilled in the art at the time of invention would have been motivated provide the result of the XOR operation in less time.

(10) Response to Argument

The appellant has presented 3 different issues, the examiner has selected claim 1 to be representative of Issue #1, claim 16 to be representative of Issue #2, and claim 17 to be representative of Issue #3.

Issue #1

The appellant argues that it is far from obvious to combine Fig. 5 of Childs with Fig. 18.6 of Schneier to obtain Fig. 1 of the application, and that that there is no suggestion that the SHA-1 and MD5 circuitry of Ober can share the same circuitry. First of all, the examiner points out that independent claim 1 does not recite all of the circuitry depicted in Fig. 1 of the application and therefore all the circuitry is not required in order to meet the limitations of claim 1. Secondly, although Ober does not specifically state that MD5 and SHA-1 circuitry are shared, Ober does clearly show that at least some of the circuitry is shared. This can clearly be seen in Col. 38 Lines 26-39 and Col. 39 Lines 14-19 where there is only one input buffer (Element 116 of Fig. 9) that is used for all MD5 and SHA-1 hashing. Therefore, Ober suggest that circuitry can be

shared between the MD5 and SHA-1 circuits. Furthermore, it was well within the ordinary skill in the art to have recognized the portions of the circuitry that were the same in SHA-1 and MD5, and the portions of the circuitry that were different, and since Ober showed that the hash circuits could share circuitry, it was reasonable to expect that one of ordinary skill in the art would have done so.

Furthermore, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). As evidenced by the previous paragraph, and the response to arguments beginning on page 9 of the Final office action dated 1/14/2005, the ordinary person skilled in the art would have found all the necessary teachings and motivation to combine the references used in the 103 rejection of claims 1 and 14 above, in the teachings of the references and from general knowledge in the art. Therefore, the examiner respectfully submits that the combination of Ober, Childs, Schneier, Turner, and Batcher in the 103 rejection of claim 1 did not apply improper hindsight.

Issue #2

The appellant argues that there is nothing to suggest that the Masaki approach of Exclusive OR through multiple input could be used in place of the feedback approach of Childs. The examiner respectfully disagrees. Col. 9 Lines 64-65 of Childs show the output of the circuitry elements 605-608, which are the feedback circuitry referred to by the appellant, to be "W[t+16] = S1 (W[t+13] XOR W[t+8] XOR W[t+2] XOR W[t])" wherein S1 is a shift of the

output of the XOR feedback circuit 605 and 606. As such, the output of the feedback circuit 605 and 606 is simply W[t+13] XOR W[t+8] XOR W[t+2] XOR W[t], which is equivalent to having a circuit with three XOR gates and four inputs (A, B, C, D) operating as such:

A XOR1 B = AxB

(AxB) XOR2 C = (AxB)xC

[(AxB)xC] XOR3 D = [(AxB)xC]xD

wherein 'x' represents the XOR operation.

This is simply repeating the XOR operation 3 separate times. Masaki clearly states in Col. 1 Lines 11-17 that "a conventional method of outputting the EXCLUSIVE-OR of a multiple input signal was to repeat many times the operation for the case of two inputs." Masaki further teaches a disadvantage of such a system is that it is time consuming. Masaki goes on to state that the circuit provided is "a MOSFET circuit with a small number of constituent elements which can speedily and simultaneously generate an EXCLUSIVE-OR output and its negation". As such, Masaki provided an alternate means for producing the same output as elements 605 and 606 of Childs, but in a less time consuming manner. Therefore, the examiner respectfully submits that Masaki more than suggests that the XOR operations of Childs can be replaced by the multiple input XOR circuit of Masaki.

Issue #3

The appellants argue that it would not be obvious for the register array to be used in common for both the MD5 and SHA-1 hashing. First, the examiner would like to point out that the claim language does not specifically state that circuitry was shared between the SHA-1 and

MD5, but rather that the circuitry was present and functioning during the operation of either algorithm. Second, as can be seen from Table 1 of Ober, there was only one set of registers supplied to the hash block, and none of the registers were specific for either MD5 or SHA-1. As such, it would be more than obvious to share the register array of Childs used for SHA-1, when performing MD5. Further, as can be seen from Childs Fig. 6, the register array 602 selects as an output a data word stored in one of the plurality of registers, specifically word 0, 2, 8, or 13, which meets the requirement of claim 15. Further, it is clear that the register array was a word wise circular queue, as can be seen in Fig. 6 Elements 601, 602, 603, 605, 607, and 608, which therefore meets the requirements of claim 17. Therefore, the examiner respectfully disagrees with the appellants argument.

To summarize, the examiner has addressed the appellant's arguments:

As per Issue #1, the examiner has addressed the appellant's arguments pertaining to the lack of motivation to combine the circuitry of Childs and Schneier. The examiner has provided support that motivation to combine these circuits did exist and therefore the combination was properly applied.

As per Issue #2, the examiner has addressed the appellant's arguments pertaining to the issue of whether the XOR circuitry of Masaki would have provided the same functionality as the feedback circuitry of Childs. The examiner has provided support that in fact both circuits would provide the result desired by Childs and that proper motivation to replace the circuit of Childs with the circuit of Masaki.

As per Issue #3, the examiner has addressed the appellant's arguments pertaining to the use of the register array for both the first and second algorithms. The examiner has shown that the claims do not require that the register array be used for both algorithms, but instead that the register array be functioning during the execution of both algorithms. Further, the examiner has shown that Ober disclosed only one set of registers to be used for both algorithms.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Matthew Henning

September 6, 2005

Conferees:

Christopher Revak 9/1/05

Ayaz Sheikh

FREESCALE SEMICONDUCTOR, INC.
LAW DEPARTMENT
7700 WEST PARMER LANE MD:TX32/PL02
AUSTIN, TX 78729